AMENDMENTS TO THE CLAIMS

1-9. (Cancelled)

10. (Currently Amended) ~~An apparatus~~A method as recited in Claim [[9]]33, wherein ~~the steps further~~ identifying first sub-entries in a first access control list comprises:

identifying a dimensional range and a policy action for each entry in the ~~second~~first access control list;

identifying all overlapping dimensional ranges in the ~~second~~first access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the ~~second~~first access control list overlap;

identifying all non-overlapping dimensional ranges in the ~~second~~first access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the ~~second~~first access control list that do not overlap dimensional ranges of other entries in the ~~second~~first access control list;

identifying a policy action for each identified overlapping dimensional range in the ~~second~~first access control list; and

identifying a policy action for each identified non-overlapping dimensional range of the ~~second~~first access control list~~; and~~

~~determining whether each identified overlapping and non-overlapping dimensional range identified from the second access control list is contained by or equal to a dimensional range of entries in the first access control list in which the entries of the first access control list have the policy action of that identified overlapping or non-overlapping dimensional range~~.

11. (Currently Amended) ~~An apparatus~~A method as recited in Claim [[9]]35, wherein ~~the steps further~~ identifying second sub-entries in a second access control list comprises:

identifying a dimensional range and a policy action for each entry in the second access control list;

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

identifying a policy action for each identified overlapping dimensional range of the second access control list; and

identifying a policy action for each identified non-overlapping dimensional range of the second access control list~~; and~~

~~wherein determining whether each identified overlapping and non-overlapping dimensional range of the first access control list is contained by or equal to a dimensional range of entries in a second access control list includes determining whether each identified overlapping and non-overlapping dimensional range identified from the first access control list is contained by or equal to overlapping and non-overlapping dimensional ranges of the second access control list~~.

12-13. (Canceled)

14. (Currently Amended) ~~An apparatus~~A method as recited in Claim [[9]]10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

15. (Currently Amended) ~~An apparatus~~A method as recited in Claim [[9]]10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

16. (Currently Amended) ~~An apparatus~~A method as recited in Claim [[9]]10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

17-32. (Cancelled)

33. (New) A method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

identifying first sub-entries in a first access control list, wherein the first access control list comprises first entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of the second access control list.

34. (New) A method as recited in Claim 33, further comprising determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is equivalent to or contained by one or more entries of the second access control list.

35. (New) A method as recited in Claim 33, further comprising:

identifying second sub-entries in the second access control list, wherein the second access control list comprises second entries, and wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and

wherein determining whether each of the first sub-entry in the first access control list

is equivalent to or contained by one or more entries of the second access control list includes determining whether the each of the first sub-entries in the first access control list is equivalent to or contained by one or more of the second sub-entries identified from the second control list.

36. (New) A computer readable medium for comparing access control lists to configure a security policy on a network, the computer readable medium carrying instructions for performing the steps of:

identifying first sub-entries in a first access control list, wherein the first access control list comprises first entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of the second access control list.

37. (New) A policy server communicatively coupled to security devices in a network to configure a security policy on a network, the policy server comprising:

a processor;

a network interface that communicatively couples the processor to the network to receive flows of packets therefrom;

a memory; and

sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of:

identifying first sub-entries in a first access control list, wherein the first access control list comprises first entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of the second access control list.

38. (New) A policy server as recited in Claim 37, wherein said sequence of instructions further comprising instructions for performing determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is equivalent to or contained by one or more entries of the second access control list.

39. (New) A policy server as recited in Claim 37,

wherein said sequence of instructions further comprising instructions for performing identifying second sub-entries in the second access control list, wherein the second access control list comprises second entries, and wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and

wherein said instructions for performing determining whether each of the first sub-entry in the first access control list is equivalent to or contained by one or more entries of the second access control list include instructions for performing determining whether the each of the first sub-entries in the first access control list is equivalent to or contained by one or more of the second sub-entries identified from the second control list.

40. (New) A policy server as recited in Claim 37, wherein said instructions for performing identifying first sub-entries in a first access control list comprise:

instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list;

instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

instructions for performing identifying a policy action for each identified overlapping dimensional range in the second access control list; and

instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

41. (New) A policy server as recited in Claim 39, wherein said instructions for performing identifying second sub-entries in a second access control list comprise:

instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list;

instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

instructions for performing identifying a policy action for each identified overlapping dimensional range of the second access control list; and

instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

42. (New) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

43. (New) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

44. (New) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

45. (New) An apparatus for comparing access control lists to configure a security policy on a network, the apparatus comprising:

means for identifying first sub-entries in a first access control list, wherein the first access control list comprises first entries, and wherein the first sub-entries identified from the first access control list comprise (i) disjoint entries of the first entries or (ii) overlapping sections identified from the first entries or (iii) non-overlapping sections identified from the first entries; and

means for programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is equivalent to or contained by one or more entries of the second access control list.

46. (New) An apparatus as recited in Claim 45, further comprising means for determining that the first access control list is functionally equivalent to the second access control

list in response to a determination that each of the first sub-entries is equivalent to or contained by one or more entries of the second access control list.

47. (New) An apparatus as recited in Claim 45,

further comprising means for identifying second sub-entries in the second access control list, wherein the second access control list comprises second entries, and wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and

wherein the means for determining whether each of the first sub-entry in the first access control list is equivalent to or contained by one or more entries of the second access control list includes means for instructions for performing determining whether the each of the first sub-entries in the first access control list is equivalent to or contained by one or more of the second sub-entries identified from the second control list.

48. (New) An apparatus as recited in Claim 45, wherein the means for identifying first sub-entries in a first access control list comprises:

means for identifying a dimensional range and a policy action for each entry in the second access control list;

means for identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

means for identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

means for identifying a policy action for each identified overlapping dimensional range in the second access control list; and

means for identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

49. (New) An apparatus as recited in Claim 47, wherein the means for identifying second sub-entries in a second access control list comprises:

means for identifying a dimensional range and a policy action for each entry in the second access control list;

means for identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

means for identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

means for identifying a policy action for each identified overlapping dimensional range of the second access control list; and

means for identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

50. (New) An apparatus as recited in Claim 48, wherein the means for identifying a dimensional range and a policy action for each entry in the first access control list includes means for identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

51. (New) An apparatus as recited in Claim 48, wherein the means for identifying a dimensional range and a policy action for each entry in the first access control list includes means for identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

52. (New) An apparatus as recited in Claim 48, wherein the means for identifying a dimensional range and a policy action for each entry in the first access control list

includes means for identifying a communication protocol for communication packets specified by each of the entries in the first access control list.